Lab # 9

*Installing Active Directory Certificate Services*



Internet Connection needs to be Established on your Virtual Machine

**Log On Information**

|  |  |
| --- | --- |
| Local Administrator | MSPress#1 |

# TERMS TO UNDERSTAND BEFORE BEGINNING LAB

|  |  |
| --- | --- |
| **Public Key Cryptography** |  |
| **Public key** |  |
| **Private Key** |  |
| **Shared Secret Key** |  |
| **Certificate Authority (CA)** |  |
| **Root (CA)** |  |
| **Intermediate CAs** |  |
| **Digital Certificate** |  |
| **Digital Signature** |  |
| **Certificate Practice Statement (CPS)** |  |
| **Certificate templates** |  |
| **Smart Cards** |  |
| **Self-enrollment** |  |
| **Auto-enrollment** |  |
| **Recovery agents** |  |
| **Key archival** |  |
| **Certification Authorities (CAs)** |  |
| **Web Enrollment** |  |
| **Online Responder** |  |
| **Network Device Enrollment Service (NDES)** |  |
| **Protocol (SCEP)** |  |
| **Standalone CA** |  |
| **Enterprise CA** |  |
| **Simple Certificate Enrollment** |  |
| **Certification Authority Web Enrollment** |  |
| **DHCP Enforcement** |  |
| **Internet Protocol Security (IPSec) enforcement** |  |
| **VPN enforcement** |  |
| **802.1X Enforcement** |  |
| **Terminal Services Gateway (TS Gateway) enforcement** |  |
| **System Health Agents (SHAs)** |  |
| **Statement of Health (SOH)** |  |
| **NAP Agent** |  |
| **System Statement of Health (SSOH)** |  |
| **Enforcement point** |  |
| **Health Registration Authority (HRA)** |  |
| **Statement of Health Response (SOHR)** |  |
| **NAP Administration servers** |  |
| **System Statement of Health Response (SSOHR)** |  |

SCENARIO: You are Network Administrator for London Accounting. The CIO has given you the task of increasing security within the London Accounting Network. As Network Administrator you understand PKI Certificates allow for secure communications with internal applications, such as intranet web servers as well as allow users to encrypt sensitive files pertaining to government tasks.

To this extent, first you need to Install and Configure Active Directory Certificate Services. (Help is found on page 246 of your textbook)

Once your Active Directory Certificate Services have been installed, your next need to Configure Certificate Revocation. (Help is found on page 248 of your text book)

Notes about Certificate Revocation: In Windows Server 2008, you can configure one or more Online Responders to make revocation information available for one or more CAs.

Why it needs to be configured: Before you can begin to deploy PKI certifications in a production environment, you need to configure certificate revocation so that your AD CS infrastructure can react appropriately to certificates that need to be revoked because an employee resigns, is terminated, or encounters a situation in which their existing private key becomes stolen or otherwise compromised.

Once you Configure Certificate Revocation you next need to Configure Certificate Enrollment.

Notes about Certificate Enrollment: You must configure your user and computer accounts to allow for PKI certificate auto enrollment, for those certificate types that do not allow for auto-enrollment, you need to use manual request mechanisms to obtain certificates for the appropriate users and computers.

Why it needs to be configured: Once you determine that your AD CS infrastructure is ready to be placed into production use on your network, you must use Certificate Enrollment to do so.

If in the case users lose their private keys associated with their PKI certificates, what would be your solution?

What did you learn in this lab?

Is there any other solution to the task your CIO asked you to complete?

Do you understand why this solution was made? If so, why? If not, see Instructor.

Notes: